SCALABLE
NETWORK TECHNOLOGIES

Cyber Security Solutions for Critical Infrastructure

Cyber threats against public utilities and other critical infrastructure are now just as common as attacks on governmental and corporate computing environments. But, instead of simply losing sensitive data, malicious attacks against power generation and distribution systems, water treatment plants, and transportation facilities can disrupt commerce and daily life across a wide area.

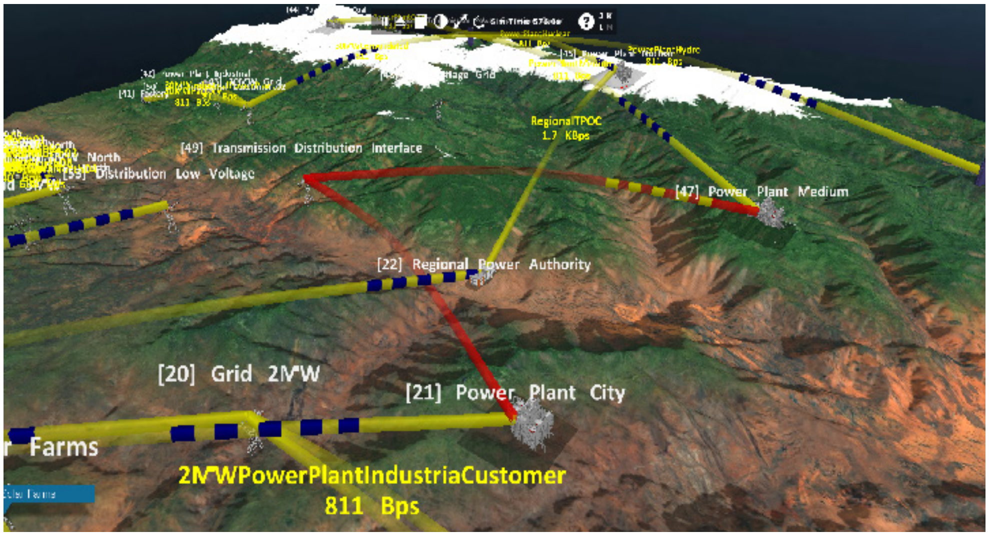
There is a pressing need for operators to determine how resilient their communications fabric is to cyber attack and to develop plans to mitigate the associated risks.

SCALABLE's high fidelity network emulation is used to simulate and predict the behavior of networked environments based on various operational scenarios, **including cyber attacks**. The emulation runs in real-time and models connections, computers, protocols, firewalls and other defenses.

SCALABLE has developed a high-fidelity network emulator, EXata CPS, to simulate the underlying communication fabric of electrical grids and test the cyber resilience of such systems. EXata CPS is integrated with OPAL-RT's HYPERSIM simulator on the same hardware (or box) to offer a complete real-time cyber-physical solution for the development, testing, and assessment of electrical grids with communication networks.

Power Generation • Water Treatment • Transportation

Critical infrastructure relies on networked communications for monitoring and control. This means they are vulnerable to cyber attacks.


RegionalTPOC
1.7 KBps
[49] Transmission Distribution Interface
North
[53] Distribution Low Voltage
[47] Power Plant Medium
[22] Regional Power Authority
[20] Grid 2MW
[21] Power Plant City
Farms
2MWPowerPlantIndustriaCustomer
811 Bps

SCALABLE Virtual Network Models enable high fidelity "what if" analysis of scenarios and risks.

SCALABLE
NETWORK TECHNOLOGIES

Benefits of EXata CPS

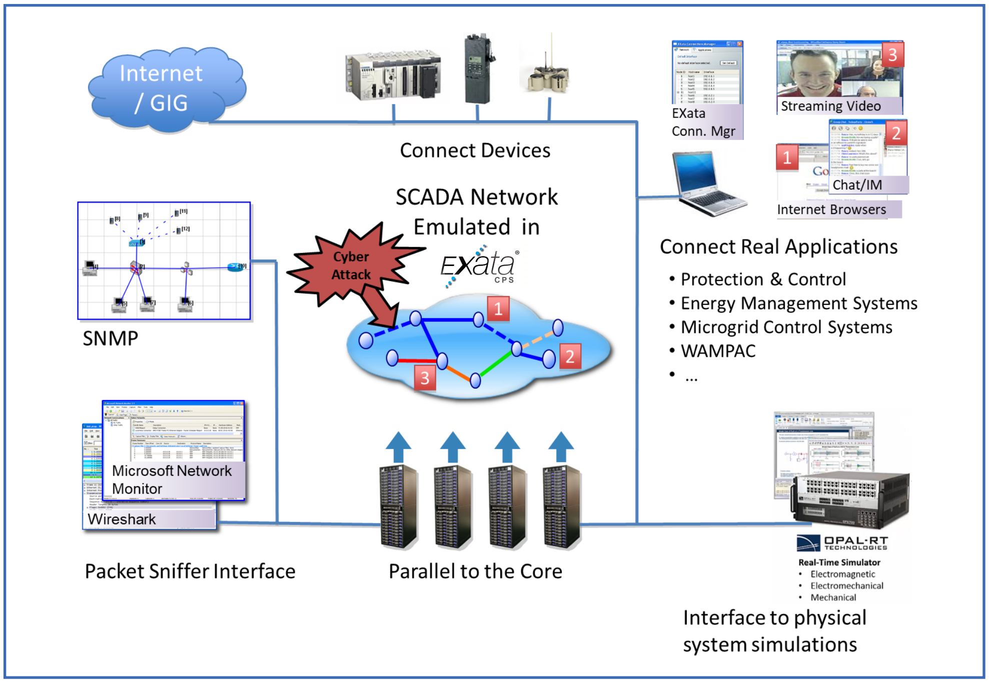
Some of the benefits of EXata CPS are:

- Integration of emulated network with equipment and physical system dynamics simulation.
- Packet-level emulation to predict system behavior under attack.
- Scalability to represent the entire network while respecting timing constraints.
- Run ‘what-if’ scenarios of control systems under cyber-attack without threatening operations.
- Assess the effectiveness of tools, techniques, and architectures to ensure system availability.
- Measure and improve system resiliency, and develop plans to mitigate risks from cyber attacks.
- Packaging of EXata CPS and HYPERSIM in the same box enables fast communication at Layer 2, ensuring that the timing constraints of the overall system can be met.

Communication Protocols Supported by EXata CPS

EXata CPS communicates with HYPERSIM by means of the following protocols:

- Generic Object-Oriented Substation Events (GOOSE), a subset of IEC61850
- C37.118 (over TCP/IP), used by synchrophasors
- DNP3 (over TCP/IP)
- Modbus (over TCP/IP)



Types of Attacks and Defenses

EXata CPS can model a number of types of attacks. The most important attacks which impact power systems are:

- Denial of Service: These attacks can bring down or make unavailable a critical piece of equipment.
- Packet Modification Attacks: These attacks make changes to the payload of packets and can result in:
  - Bogus input data, such as modified sensor data: Can lead to erroneous decisions by the controllers.
  - Bogus output data, such as manipulated or misleading data sent to controllers: Can lead to unintended or incorrect actions.
  - Disrupt time synchronization by delaying delivery: Can lead to instability in the physical system.

The other types of attacks that can be modeled in EXata CPS include:

- Passive Attacks:
  - Eavesdropping
  - Network Scanning
  - Port Scanning
  - SIGINT
- Jamming Attacks
- Vulnerability Exploitation Attacks
  - Attacks to corrupt files and databases
  - Hacking attacks
- Virus and Worm propagation attacks
- Rootkit attacks
- Botnet attacks
- Backdoors and holes in the network perimeter
- Communications hijacking and man-in the-middle attacks
- Coordinated Attacks
- Adaptive Attacks

EXata CPS can model the following types of cyber defenses:

- Firewalls: The firewall model is based on iptables. Firewall rules can be modified dynamically while the simulation is running.
- Intrusion Detection System (IDS)
- Anti-Virus System (AVS)
- Security Logs and Audit Trails